RIVISTA DI SCIENZE DELL'EDUCAZIONE

PONTIFICIA FACOLTÀ DI SCIENZE DELL'EDUCAZIONE AUXILIUM
ANNO LVI • MAGGIO/AGOSTO 2018

DOSSIER
GIOVANI DONNE:
ASPIRAZIONI RISORSE
FRAGILITÀ'

2018/2

RSE

POSTE ITALIANE SPA - SPED. IN ABB. POSTALE D.L. 353/2003 (CONV. IN L. 27/02/2004 N. 46) ART. 1, COMMA 1 E 3, C/RM/04/2014

RIVISTA DI SCIENZE DELL'EDUCAZIONE

PUBBLICAZIONE QUADRIMESTRALE
EDITA DALLA PONTIFICIA
FACOLTÀ DI SCIENZE DELL'EDUCAZIONE
"AUXILIUM" DI ROMA

DIREZIONE
Via Cremolino 141
00166 Roma

Tel. 06.6157201
Fax 06.615720248

E-mail
rivista@pfse-auxilium.org
coordinatore.rse@pfse-auxilium.org

Sito internet
http://rivista.pfse-auxilium.org/

Informativa GDPR 2016/679
I dati personali non saranno oggetto di comunicazioni o diffusione a terzi. Per essi Lei potrà richiedere, in qualsiasi momento, accesso, modifiche, aggiornamenti, integrazioni o cancellazione, rivolgendosi al responsabile dei dati presso l'amministrazione della rivista.

ASSOCIATA
ALLA UNIONE STAMPA
PERIODICA
ITALIANA

Aut. Tribunale di Roma
31.01.1979 n. 17526

Progetto grafico impaginazione
e stampa
EMMECIPI SRL

ISSN 0393-3849

RIVISTA DI SCIENZE DELL'EDUCAZIONE

ANNO LVI NUMERO 2 • MAGGIO/AGOSTO 2018

Poste Italiane Spa
Sped. in abb. postale d.l. 353/2003
(conv. in L. 27/02/2004 n. 46) art. 1, comma 2 e 3, C/RM/04/2014

PONTIFICIA FACOLTÀ DI SCIENZE DELL'EDUCAZIONE AUXILIUM

SOMMARIO

DOSSIER

GIOVANI DONNE: ASPIRAZIONI, RISORSE, FRAGILITÀ

Young women: aspirations, resources, fragility

SISTEMA PREVENTIVO OGGI

ALTRI STUDI

ORIENTAMENTI BIBLIOGRAFICI

RIVISTA DI SCIENZE DELL'EDUCAZIONE

PONTIFICIA FACOLTÀ DI SCIENZE DELL'EDUCAZIONE AUXILIUM

ALTRI STUDI

RSE

IL FATTORE UMANO NELLA SICUREZZA INFORMATICA: IL RUOLO CHIAVE DELLA CONSAPEVOLEZZA

THE HUMAN FACTOR IN INFORMATION SECURITY: THE KEY ROLE OF UNDERSTANDING

ISABELLA CORRADINI[1]

Lo scenario digitale nel quale ci si muove è in continua evoluzione, considerato che i temi dell'Intelligenza Artificiale e dell'Internet delle Cose (*Internet of Things*, IoT) avranno uno spazio e un'attenzione sempre maggiori.
Le tecnologie digitali pervadono la vita di tutti e non possono essere considerate (almeno non più) come qualcosa di esterno all'individuo. Sarebbe in proposito opportuno evitare l'uso del termine virtuale quando si fa riferimento ai comportamenti in Rete, dal momento che le azioni sono reali al pari delle conseguenze prodotte.
La persona, ovvero il fattore umano, si muove in un continente complesso e articolato che apre almeno a tre considerazioni.
La prima è che tutti (o quasi), indipendentemente dall'età, ci troviamo immersi in una realtà che comporta tanti vantaggi ma, al contempo, espone a diversi rischi, da quelli relativi alla profilazione mediante i *Big Data*, alla gestione in sicurezza dell'identità digitale. Se è vero che le nuove generazioni saranno sempre più digitali, non per questo potranno considerarsi esenti da tali rischi.
La seconda è che la possibilità di avere tutto il mondo in tasca grazie ad uno *smartphone* rende sempre meno marcati i confini tra contesto privato e lavorativo, tranne quelli che, con molta fatica, l'essere umano riesce a mantenere.
Infine, questo scenario risulta essere molto articolato per lo sviluppo dell'IoT, dove si assiste alla fusione tra mondo fisico e virtuale. Le previsioni indicano che saranno miliardi gli oggetti dotati di sensori connessi in Rete che andranno ad influenzare diversi settori del quotidiano, dal commercio al sistema bancario, alla vita privata dell'individuo. Nel frattempo si parla già dell'Internet di tutte le cose (*Internet of Everything*, IoE).
Tuttavia, nonostante i benefici di queste tecnologie digitali, già da tempo gli esperti di sicurezza Information Technology (IT) hanno allertato sui rischi dell'IoT: la connessione tra i due mondi, infatti, e la mole di dati prodotti, costituiscono

un'attrattiva per i cybercriminali, a fronte anche di un'oggettiva impossibilità di garantire la sicurezza di tutti i dispositivi interconnessi.
Spesso, purtroppo, nel delineare le strategie di intervento, si sottovaluta l'importanza del fattore umano che, invece, se informato e formato in modo adeguato, può costituire l'elemento vincente della sicurezza di ogni organizzazione.
Il presente articolo si focalizza sull'importanza del fattore umano nella sicurezza informatica (*cybersecurity*) e sulla necessità di adottare comportamenti consapevoli nell'uso delle tecnologie digitali. Esse, infatti, non sono né buone né cattive: la differenza consiste nell'uso che ne fanno le persone.

1. Comportamenti rischiosi ed ingegneria sociale

Diversi rapporti pubblicati annualmente sulla sicurezza informatica[2] sottolineano come l'anello debole della *cybersecurity* sia rappresentato dal fattore umano. Il Rapporto 2018 sulle violazioni dei dati (*data breach*) pubblicato da Verizon,[3] ad esempio, evidenzia la necessità di continuare ad investire su programmi di formazione nelle aziende, dal momento che l'essere umano è tra le principali vulnerabilità sfruttate dai cybercriminali. Basta, infatti, che un dipendente di un'azienda cada nel tranello di una mail *phishing* per compromettere la sicurezza aziendale.
Il *phishing* è un tipo di frode *online* che consiste nell'invio di una mail esca agli utenti - generalmente fingendosi organizzazioni riconosciute - con lo scopo di indurre la vittima a fornire informazioni sensibili, come numeri di carta di credito, password, ecc. Combinando il carattere di urgenza con la naturale curiosità umana, l'utente, soprattutto in condizioni di fretta o di distrazione, viene indotto ad aprire link o allegati malevoli: nel più fortunato dei casi si tratta solo di spam, negli altri invece si scarica un malware[4] che infetta il sistema operativo. Talvolta queste mail sono molto più mirate, vale a dire che, invece di essere inviate ad una moltitudine di persone come accade nel caso del *phishing*, sono recapitate a target specifici (utenti e aziende). In questo caso si parla di messaggi di *spear phishing* e la difficoltà a riconoscerli sta nel fatto che sembrano provenire da un indirizzo conosciuto.
Nei messaggi, inoltre, si fa spesso riferimento a dettagli personali dell'utente, come ad esempio un compleanno, un acquisto effettuato di recente. Ovviamente, dietro queste attività mirate c'è spesso uno studio delle abitudini e del comportamento del soggetto target, per far sì che egli possa essere attratto dalla familiarità delle parole contenute nella mail e compiere delle azioni ad esclusivo vantaggio dell'ingegnere sociale.
Gli esempi descritti, infatti, rientrano nel campo dell'ingegneria sociale *(social engineering)* che, in sintesi, mira a sfruttare le relazioni umane per ottenere informazioni. Si tratta di una forma di *hacking* cognitivo (*cognitive hacking*),[5] ovvero un tipo di attacco

RIASSUNTO

Il presente articolo si focalizza sull'importanza del fattore umano nella sicurezza informatica (*cybersecurity*) e sulla necessità di adottare comportamenti consapevoli nell'uso delle tecnologie digitali. Esse, infatti, non sono né buone né cattive: la differenza consiste nell'uso che ne fanno le persone.

Parole chiave

Cybersecurity, ingegneria sociale, fattore umano, tecnologie digitali, *cybercrimine*, consapevolezza.

SUMMARY

The present article focuses on the importance of the human factor in information security (*cybersecurity*) and on the necessity of adopting behavior that is aware of the use of digital technology. In fact, it is neither good or bad: the difference consists in the use people make of it.

Key words

Cybersecurity, social engineering, human factor, digital technology, *cybercrime*, awareness.

RESUMEN

El presente artículo se refiere a la importancia del factor humano en la seguridad informática (*cybersecurity*) y a la necesidad de adoptar comportamientos conscientes en el uso de las tecnologías digitales. Estas no son, en sí mismas, ni buenas ni malas: la diferencia consiste en el uso que de ellas hacen las personas.

Palabras clave

Seguridad informática, ingeniería social, factor humano, tecnologías digitales, *crimen informático*, consciencia.

non tecnologico la cui riuscita è legata specificamente al cambiamento del comportamento degli utenti, indotto manipolandone la percezione. L'ingegnere sociale non ha necessariamente competenze informatiche: il suo *modus operandi* è basato soprattutto sulle sue capacità di creare empatia e di trasformare la sfiducia dell'interlocutore in fiducia.[6]

La riuscita di queste tecniche si basa sull'applicazione di principi psicologici noti nell'ambito della psicologia sociale[7] e sulle euristiche, vale a dire strategie cognitive mediante le quali le persone elaborano giudizi, prendono decisioni, senza impegnare troppe risorse mentali.

Non di rado, infatti, l'elaborazione delle informazioni avviene senza prendere in considerazione tutti i fattori della situazione. Così, ad esempio, la familiarità, la simpatia, il bisogno di aiuto diventano leve strategiche che sulle quali l'ingegnere sociale può agire nel suo esclusivo interesse. Oltre al *phishing* e alle tecniche di ingegneria sociale, ci sono poi altri

comportamenti umani che possono compromettere la sicurezza dei propri dati e di quelli dell'organizzazione nella quale si lavora. Se, ad esempio, si usano account personali invece di quelli aziendali, va da sé che si pongono questioni di sicurezza, oltre che di credibilità. Non è un caso che le aziende stanno adottando politiche sempre più stringenti riguardo l'utilizzo di dispositivi e account rigorosamente aziendali, proprio perché ad essi sono dedicate specifiche protezioni da parte dei settori IT.

C'è poi il tema della gestione delle *password*, un vero e proprio lavoro cognitivo e non certo banale, dal momento che bisogna sceglierle "robuste" e aggiornarle. E nemmeno replicarle nei molti account che si possiedono. Secondo i rapporti diffusi annualmente da Keeper Security,[8] dall'analisi di milioni di stringhe diventate pubbliche a causa di violazioni di dati (*data breach*) la *password* più diffusa continua ad essere "123456".

Nel corso degli anni, l'elenco delle *password* utilizzate più di frequente non sembra avere avuto grandi cambiamenti. Sebbene gli esperti di sicurezza segnalino come la gestione delle *password* sia un'attività di vitale importanza per la sicurezza informatica, non tutti dedicano tempo e risorse (anche cognitive) a tale compito.

2. Ossessione della condivisione e impatti sociali

Il *web* è disseminato di ami, come le mail di *phishing,* e di tracce: queste sono rappresentate da tutte le informazioni che si lasciano in Rete, che si tratti di un acquisto fatto o di notizie postate su un profilo *social*. Queste tracce raccontano di noi, di chi siamo, di cosa facciamo, di cosa preferiamo. Basti pensare alla localizzazione delle mappe di *Google* o ai *like* lasciati sui vari *social media*. Tutte queste informazioni contribuiscono alla creazione di veri e propri profili reputazionali, utilizzati con l'obiettivo di indirizzare mirate attività di marketing, che saranno sempre più gestite in modo automatico grazie ai continui progressi delle tecniche di Intelligenza Artificiale.[9]

Sotto il profilo della sicurezza, è evidente che il problema sta nei dati che si immettono e si condividono in Rete. In particolare, si osserva come ormai sui *social* viene pubblicato di tutto, dalla scelta delle vacanze ai dettagli della propria vita personale, senza porsi il problema che il pubblico della Rete, pur essendo invisibile, può essere particolarmente numeroso e con interessi diversi. C'è dunque anche chi vi trova lo strumento privilegiato per la realizzazione di attività illecite e criminose. Si pensi, ad esempio, al fenomeno della pedopornografia online, che sfrutta le foto di minori diffuse via *web*. Il desiderio di condividere i momenti felici della nascita e dei primi anni dei propri figli, purtroppo rischia di trasformarsi in un problema serio per la *privacy* e la sicurezza dei minori.

Senza contare che la condivisione di foto e video in Rete può costituire una vera e propria ossessione, al

punto che è stato coniato il termine di *sharenting.*[10]

Il problema riguarda non solo le generazioni di giovani, ma anche di adulti. Si è ormai talmente immersi nel vasto universo dei *social media* che perfino l'evento reale viene vissuto in differita: non sono pochi coloro che, invece di godersi appieno le emozioni di un concerto o di una cena tra amici, preferiscono passare il tempo a documentare tutto l'evento con *post* e *tweet*.

Catturati dal proprio *smartphone* non ci si accorge più dell'"altro"; non mancano casi di cronaca in cui, invece di prestare aiuto a persone in difficoltà, si è preferito continuare a fotografare e filmare per poi avere lo *scoop* da mettere in Rete.

Il punto focale sul quale riflettere è il paradosso del rapporto che si è instaurato con le tecnologie digitali: da un lato esse hanno cambiato il modo di lavorare e creato nuove opportunità di comunicare e socializzare; dall'altro, soprattutto per i più giovani, sembra invece che ad essere preferita sia la relazione *online* piuttosto che quella *offline* (di persona). Inoltre, va osservato che un "legame emotivo" troppo stretto con il proprio dispositivo può condurre a stati di malessere: la ricchezza degli stimoli prodotti da uno *smartphone*, infatti, può essere così assorbente da soffrirne quando si è impossibilitati ad usarlo, condizione nota con il nome di nomofobia.[11]

Tali considerazioni non devono condurre ad una demonizzazione delle tecnologie digitali, perché sono comunque portatrici di vantaggi, ma occorre essere consapevoli dei rischi ai quali un loro uso sconsiderato può esporre. Rischi che vanno ben oltre la sicurezza informatica e che riguardano prima di tutto il benessere dell'individuo e la salvaguardia delle relazioni umane.

3. Educare alla consapevolezza

Dal momento che i cittadini sono utilizzatori delle tecnologie digitali sia nel privato che in ambito lavorativo, va da sé che il tema della sicurezza informatica non può essere considerato di esclusivo interesse per i soli specialisti del campo.[12]

Le minacce evolvono, le tecnologie pure ed il problema va affrontato con un approccio olistico, se si vogliono ottenere risultati efficaci.

Di conseguenza, a parte il contributo delle soluzioni tecnologiche, indispensabili ma non risolutive, occorre adoperarsi seriamente per lo sviluppo di una cultura della sicurezza volta ad incrementare la sensibilità verso una maggiore conoscenza delle minacce informatiche: una maggiore confidenza con l'ambiente *online*, infatti, permette di comprenderne i pericoli e gestirli di conseguenza. Sviluppare la cultura della sicurezza richiede però di intervenire in modo differenziato a seconda dei destinatari, con la progettazione di attività che vanno dalla sensibilizzazione alla formazione e l'impiego di strumenti e metodologie didattiche specifici.

Nella pratica quotidiana si assiste

spesso all'utilizzo di parole sicuramente attrattive, come quella di *awareness* per indicare la consapevolezza, ma che poi devono tradursi in efficaci programmi di intervento. Ad esempio, per quanto riguarda l'ingegneria sociale, è fondamentale che le persone acquisiscano consapevolezza delle tecniche usate dai cybercriminali e sviluppino la capacità di elaborare dei punti di attenzione.[13]

In un'ottica più estesa, dal momento che l'approccio alle tecnologie digitali è sempre più precoce, è bene cominciare fin dalla scuola il percorso di educazione al loro uso consapevole. Allo scopo è possibile sviluppare progetti e programmi volti a favorire un'adeguata conoscenza del mondo digitale con cui bambini e ragazzi interagiscono.

In questa direzione si muovono alcuni interessanti progetti, tra i quali "Programma il Futuro",[14] iniziativa promossa dal MIUR (Ministero dell'Istruzione, Università e Ricerca) e realizzata dal CINI (Consorzio Interuniversitario Nazionale per l'Informatica) che ha lo scopo di diffondere lo sviluppo del *pensiero computazionale* attraverso la programmazione (*coding*) in un contesto di gioco.

Il Progetto permette di sviluppare consapevolezza sugli aspetti più scientifici e culturali dell'informatica, il cosiddetto pensiero computazionale.[15] Il messaggio di fondo, infatti, è che bisogna imparare a diventare un consumatore consapevole e responsabile delle tecnologie. In altre parole: non usare il tuo telefono solo per giocarci, programmalo!

Recentemente, per rispondere alle esigenze formative degli insegnanti, nel Progetto è stata avviata un'area didattica dedicata all'uso consapevole delle tecnologie digitali.

Una recente indagine, infatti, che ha coinvolto gli insegnanti partecipanti all'iniziativa, ha fatto emergere tre importanti aspetti:[16] il ruolo svolto da genitori e insegnanti nel favorire l'uso consapevole delle tecnologie digitali; la scarsa consapevolezza dei rischi ai quali gli studenti sono esposti (bullismo, molestie, truffe, ecc.); la necessità di promuovere iniziative formative per rafforzare la conoscenza ed il senso di responsabilità legate al loro uso.

Lavorare sulla consapevolezza è quindi necessario non solo per rispondere ai bisogni di sicurezza, ma anche perché permette di far comprendere e sfruttare appieno le tante opportunità offerte dalle tecnologie digitali, alle quali non bisogna rinunciare.

Conclusione

Lo scenario digitale è in continua evoluzione ed occorre essere in grado di cogliere tutti i benefici possibili e gestire i rischi che ne derivano.

La sicurezza informatica non può funzionare delegando alle sole tecnologie il ruolo di risolutore. Ne sono testimonianza i risultati dei vari rapporti sulla sicurezza che indicano come gli incidenti e gli attacchi informatici, con vittime più o meno illustri, siano in costante aumento e sempre più specializzati. Nell'ottica di una stra-

tegia olistica non può essere assolutamente trascurato il fattore umano, soprattutto alla luce dello sviluppo dell'Internet delle cose e dei progressi dell'Intelligenza Artificiale.
Qualunque tecnologia, infatti, anche la più avanzata, rischia di essere inefficace in mano a persone non consapevoli dei rischi e delle minacce.

NOTE

[1] Psicologa sociale esperta di fattore umano nella sicurezza, *safety, security* e *cybersecurity*, e di comunicazione aziendale. È presidente e direttore scientifico di *Themis*, Centro ricerche socio-psicologiche e criminologico-forensi e co-fondatore (con il Prof. Enrico Nardelli) del *Link&Think Research Lab*, focalizzato sugli aspetti socio-tecnici delle tecnologie dell'informazione e dell'educazione informatica (pensiero computazionale). Già docente di Psicologia sociale e di psicologia del comportamento criminale presso l'Università degli Studi dell'Aquila, insegna in corsi specialistici e master universitari, tra i quali il Master in Intelligence Economica ed il corso di perfezionamento in Security Manager presso l'Università di Roma Tor Vergata. Coordina le attività di monitoraggio, di comunicazione e dell'area "uso consapevole delle tecnologie digitali" di Programma il Futuro, progetto realizzato dal Consorzio Interuniversitario Nazionale per l'Informatica (CINI) per conto del Ministero dell'Università e della Ricerca (MIUR) con l'obiettivo di diffondere la cultura informatica nelle scuole. Autrice di numerose pubblicazioni nazionali e internazionali, cura una collana sul tema della reputazione per la casa editrice Franco Angeli.

[2] Si vedano, ad esempio, i Rapporti del CLUSIT (Associazione Italiana per la Sicurezza Informatica) in https://clusit.it/rapporto-clusit/ (22-04-2018).

[3] Cf 2018 Data Breach Investigations Report (DBIR), in https://www.verizonenterprise.com /resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf, 1-8 (22-04-2018). Nel rapporto sono stati analizzati più di 53.000 attacchi e oltre 2.000 violazioni in 65 Paesi.

[4] *Malware* indica un programma in grado di produrre danni al Pc di chi lo utilizza. In questa categoria rientra anche il *ransomware*, che impedisce alla vittima di accedere al sistema del computer se non procede al pagamento di un riscatto (*ransom*). L'attacco si diffonde soprattutto via mail, mediante un allegato (es. un documento, un'immagine).

[5] Cf Cybenko George - Giani Annarita - Thompson Paul, *Cognitive hacking: A battle for the mind,* in *Computer* 35(2002)8, 50-56.

[6] Cf Corradini Isabella - Franchina Luisa, *Ingegneria sociale: aspetti umani e tecnologici*, Roma, Edizioni Themis 2016.

[7] In particolare ci si riferisce ai sei principi di cui parla lo psicologo sociale Robert Cialdini che, applicati spesso in modo automatico ed inconscio, guidano le azioni umane. I sei principi sono: reciprocità, coerenza, simpatia, autorità, scarsità e riprova sociale. Si veda, ad esempio, Cialdini Robert B., *Le armi della persuasione. Come e perché si finisce col dire di sì*, Milano, Giunti 2005.

[8] Keeper Security è una società creatrice di software per la gestione delle password. Cf https://keepersecurity.com/it_IT/ (22-04-2018).

[9] Cf Corradini Isabella (a cura di), *Internet delle cose. Dati, sicurezza e reputazione*, Milano, Franco Angeli 2017.

[10] Termine nato dalla combinazione di *parenting* e *sharing*. Indica l'uso abituale dei *social media* da parte di genitori per condividere immagini e notizie sui propri figli, dalla nascita ai primi passi, ai compleanni, ecc. È stato introdotto nel dizionario inglese Collins. Cf https://www.collinsdictionary.com/it/dizionario/inglese/sharenting (22-04-2018).

[11] Forma di dipendenza, caratterizzata dalla paura incontrollata di rimanere sconnessi dal proprio cellulare. Il neologismo, abbreviativo di *no-mobile-phone*, è apparso nel 2008 a se-

guito di una ricerca condotta nel Regno Unito dall'Ente di ricerca YouGov.

[12] Cf Corradini Isabella, *Le buone pratiche nella cybersecurity: fattore umano ed awareness*, in *ICT Security Magazine* (2015) n.127, in https://www.ictsecuritymagazine.com/articoli/le-buone-pratiche-nella-cybersecurity-fattore-umano-ed-awareness/ (22-04-2018).

[13] Cf Id., *Human factors in hybrid threats: the need for an integrated view*, in CESMA Working Group on Hybrid Threats (Ed.), *Hybrid Cyber Warfare and the evolution of aerospace power: risks and opportunities*, I Quaderni del Cesma, Roma, Associazione Arma Aeronautica 2017, 85-96.

[14] Cf il Sito del Progetto *Programma il Futuro,* in http://www.programmailfuturo.it (22-04-2018).

[15] Sul tema si veda, ad esempio, Lodi Michael - Martini Simone - Nardelli Enrico, *Abbiamo davvero bisogno del pensiero computazionale*?, in *Mondo Digitale* (novembre 2017), in http://mondodigitale.aicanet.net/2017-5/articoli/MD72_02_abbiamo_davvero_bisogno_del_pensiero_computazionale.pdf, 1-15 (22-04-2018).

[16] Gli esiti dell'indagine, realizzata dal Centro Ricerche Themis, sono basati sull'analisi di 2.422 risposte di insegnanti di ogni ordine e scuola, con una larga rappresentanza della primaria (59% dei partecipanti). Pur avendo di fatto rilevato le percezioni degli insegnanti, va comunque osservato che molti docenti hanno una lunga esperienza di insegnamento (l'87% ha più di 10 anni di esperienza) e sono pertanto in grado di valutare e riportare in modo affidabile la situazione che vivono con i propri studenti. L'indagine è scaricabile al link https://themiscrime.com/it/attivita/ricerche/item/271-indagine-themis-sull-uso-consapevole-delle-tecnologie-digitali (22-04-2018).